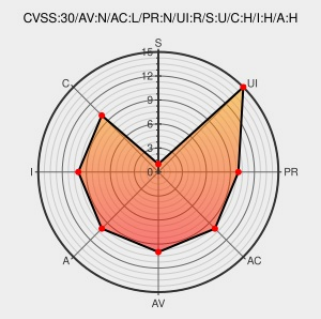
CVE-2014-0158

Published on: 04/10/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:55 PM UTC

CVE-2014-0158

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Opensuse from Opensuse contain the following vulnerability:

Heap-based buffer overflow in the JPEG2000 image tile decoder in OpenJPEG before 1.5.2 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted file because of incorrect j2k_decode, j2k_read_eoc, and tcd_decode_tile interaction, a related issue to CVE-2013-6045. NOTE: this is not a duplicate of CVE-2013-1447, because the scope of CVE-2013-1447 was specifically defined in http://openwall.com/lists/oss-security/2013/12/04/6 as only "null pointer dereferences, division by zero, and anything that would just fit as DoS."

CVE-2014-0158 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 6.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link

Bug 1082925 – openjpeg: Heap-based buffer overflow in JPEG2000 image tile decoder	Issue Tracking Third Party Advisory bugzilla.redhat.com text/html	MISC bugzilla.redhat.com/show_bug.cgi?id=1082925
Bug 871412 – VUL-0: CVE-2014-0158: openjpeg: heap-based buffer overflow in JPEG2000 image tile decoder	Issue Tracking Third Party Advisory bugzilla.suse.com text/html	MISC bugzilla.suse.com/show_bug.cgi?id=871412

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Opensuse	Opensuse	12.3	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Opensuse	Opensuse	12.3	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Application	Uclouvain	Openjpeg	All	All	All	All
Application	Uclouvain	Openjpeg	All	All	All	All

cpe:2.3:o:opensuse:opensuse:12.3:*:*:*:*:*:*:*:

cpe:2.3:o:opensuse:opensuse:13.1:*:*:*:*:*:*:*:

cpe:2.3:o:opensuse:opensuse:12.3:*:*:*:*:*:*:*:

cpe:2.3:o:opensuse:opensuse:13.1:*:*:*:*:*:*:*:

cpe:2.3:a:uclouvain:openjpeg:*:*:*:*:*:*:*:*:

cpe:2.3:a:uclouvain:openjpeg:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report